Task Proposal Request for
System Administration and Security

The Contractor must provide system administration of the SO system located at FinCEN's Vienna location. The system must be operational 24 hours per day, 7 days per week (24/7), accommodate peak operation times, ensure quick system response times (as determined herein), and ensure the system remains secure.

In performance of this task, the Contractor must:

- ?? provide training support, upgrade support, product configuration, configuration management, testing, documentation, monitoring, problem resolution, system adjustments and optimization, and 24/7 (including all federal, state, local and national holidays) operability;
- ?? ensure that SO capabilities are enhanced so that the system is reliable and capable of supporting up to 10,000 new users over the next two to three years at a potential rate of up to 500 new accounts per month;
- ?? add new users to the system and delete users within 48 hours with emergency user deletions will be handled within 2 hours;
- ?? integrate new data sources, update web content and provide redundancy to ensure 24/7 operability; and
- ?? reconcile backup logs daily to ensure complete backups are attained. On a monthly basis, perform complete restoration from backup on development server where applicable. If no development server is available for a particular application, list files from backup and ensure they are complete and the files are not corrupted.
- ?? Also included in this task is the project management to oversee all IT aspects of the SO and Gateway web system. The Project Manager oversees the systems administration and security, help desk, and the web system development and maintenance. The Project Manager handles administrative functions of the project and is responsible for the overall management of the specific task orders and insuring that the technical solutions and schedules in the task order are implemented in a timely manner.

Routine maintenance will be performed during non-peak hours (peak hours for SO are from 7 a.m.-8 p.m. EST Monday through Friday). Prior to any downtime (system or any part of the system inaccessible to users or any subset of users) or system changes, the Contractor must: 1) request permission from the COTR via email 7 workdays in advance, 2) once permission is received from the COTR via email, provide a one workweek (5 day) notification timeframe to system users, 3) provide a warning banner on all affected entry points (SO, Direct Net) which must remain in place for one workweek, and 4) provide alternate site directions to a static screen that indicates the site is down or to help screens for changes.

The Contractor is responsible for all aspects of system administration, which include, but is not limited to, implementing software upgrades, debugging, placing service calls as needed, troubleshooting, and software functionality. To perform hereunder, Contractor personnel must:

- ?? have experience with maintaining a production environment for JAVA web-based applications;
- ?? maintain required hardware and software which shall include but are not limited to: iPlanet Web Server, iPlanet Messenger, iPlanet Application Server, Windows 2000 Server, web-based 3270 terminal emulation products, Raptor firewalls, SSL acceleration, load balancing, Citrix servers, T1 lines, link controllers, network analyzers, VPNs, digital certificates, F5 Big-IP, Sun Solaris, JDBC connections to SQL databases, IBM WebSphere Application Server, web portal, and security intrusion detection products;
- ?? monitor and provide statistics regarding system availability, maintenance & upgrade schedules, system problems and/or service calls placed; and
- ?? provide documentation of system adjustments, optimizations, and additions, and documentation must be technically detailed and in-depth. The Contractor may in no way obligate the government.

All software and hardware upgrades will be government furnished. The Contractor must upgrade software to the latest level, ensuring compatibility and interoperability with other software.

The Contractor must coordinate through the COTR with the FinCEN Information Systems Security Officer (ISSO) on all security matters. Work performed must comply with the Federal Information Security Management Act of 2002 (FISMA) requirements. The Contractor must ensure and maintain government required FISMA system certification and accreditation (C&A) according to the National Information Assurance Certification and Accreditation Process (NIACAP). The Contractor must manage, maintain, upgrade, monitor and keep secure the SO system. This includes, but is not limited to, providing: 1) protection for all SO system hardware, software, and database connections, 2) providing monitoring of firewall, intrusion, and virus detection software alerts, 3) ensuring system and data integrity, and 4) taking corrective actions to secure the system from unauthorized penetration of any kind. The FinCEN ISSO will be the certifying authority for systems security, software applications, and encryption methodology. The Contractor will follow the processes and procedures provided by the FinCEN ISSO for initial registration, set-up and vetting of users.

SO documentation includes, but is not limited to the following: SO Administrative Guide, SO Security Plan, SO Network Diagram, Entity Relationship Diagrams, and Data Flow Diagrams.

Order Type: Time-and-Materials or Labor-Hours

PERFORMANCE REQUIREMENTS SUMMARY

Desired Outcome	Required Service	Performance Standard	Monitoring Method	Incentive/Disincentive
System Administration	Primary focus is system access, speed, and functionality for users. This includes system software installation and upgrades, adding user accounts, monitoring the system for uptime, debugging and correcting problems.	Complete Secure Outreach system (including 3270 emulator to DCC) accessible to users 100% of the time 7 a.m. – 8 p.m. EST Monday thru Friday, 99% at all other times. Contractor maintains Government specified system access and response time metrics and submits these to the COTR in a weekly report. System problems are immediately brought to the COTR's attention. Senior Systems Administrator is on call 24/7 and responsible for correcting system problems and outages. System problems are rectified the same day. System problems and outages are corrected the same day.	Review system metrics report and verify. Obtain and analyze user feedback. Review user complaints/trouble tracking, noting problem areas.	Full payment for 100% compliance. Payment less than 100% may be made for less than full compliance if less than full performance is accepted. For each system problem or outage not corrected the same day, a .5% deduction of the total task order monthly price will be taken for each day the system remains not fixed. System problems and outages caused by the Contractor due to error, poor planning, lack of employee coverage, will result in a 1% per day deduction of the total task order monthly price for each day (24 hours) the system remains not fixed. The Government may terminate the contract for default if the Contractor is unable to produce a solution that makes the system meet functional and system requirements within 6 workweeks of problem onset.

Desired Outcome	Required Service	Performance Standard	Monitoring Method	Incentive/Disincentive
Provide Security for the Secure Outreach	Provide technical security for the web system including: alerts, firewall monitoring, virus protection, and maintain C&A security cert.	Work performed complies with FISMA requirements. SBU security level maintained 100% of the time. C&A security level and certification maintained. Secure Outreach System detects and stops 100% virus, intruder, and other attacks. Document systems and network security processes and procedures, incident reports, and quarterly system and network vulnerability, and risk assessments. System, web, and data integrity is maintained 100% of the time.	Review work performed to ensure complies with FISMA and C&A requirements. Review work reports, incident reports, and system assessments. Review user complaints/trouble tracking, noting problem areas. Review of systems and network security processes and procedures, incident reports within three days of incident, and quarterly assessments.	Full payment for 100% compliance. For each day that the Secure Outreach system is not compliant with FISMA and C&A requirements, a 1% reduction of the total task order monthly price shall be taken. For each incidence of negative system impact caused by an unauthorized intrusion, attack or virus, a deduction from the monthly price will be based on the severity of the impact as follows: Severe (system or part of system inaccessible and destroyed and/or corrupted) – 1.5% reduction; Moderate (system or part of system inaccessible but restored within 2 days) – 1% reduction; Low (system attacked but restored within the same day) - .5%